1.Datos Generales de la asignatura

Nombre de la asignatura:	Hackeo Ético
Clave de la asignatura:	TSB-1904
SATCA[4]:	2 – 3 – 5
Carrera:	Ingeniería en Sistemas Computacionales

2.Presentación.

Caracterización de la asignatura

- Esta asignatura permite al egresado aplicar conocimientos tecnológicos en el área de las TICs, para la solución de problemas, así como apoyar en la administración de computadoras considerando el diseño, selección, instalación y mantenimiento para la operación eficiente de los recursos informáticos; desempeñándose profesionalmente con ética y respetando el marco legal.

- La asignatura es importante ya que permitirá formar especialistas en seguridad de TICs, con habilidades en hackeo ético, con el fin de incrementar la seguridad en la infraestructura, información y activos tecnológicos, ante ataques dentro y fuera de la organización.

- Esta asignatura consta de 6 temas, el primero de ellos introduce al discente en el área del hackeo ético. El segundo tema define el rastreo de huellas, así como las herramientas para efectuarlo. El tema tres contempla el hackeo a redes locales, inalámbricas, servidores y aplicaciones WEB. En el tema cuatro se aborda los tipos de malware y las herramientas para detectarlo. Las técnicas de hackeo tradicionales son tratadas en el tema 5. El tema seis contiene una introducción a las pruebas de penetración.

- Se relaciona con las asignaturas de *Seguridad Perimetral* y Criptografía ya que en ellas se discuten y analizan las estrategias de seguridad que un administrador de TICs debe implementar, y la asignatura que nos ocupa define una serie de

[4] Sistema de Asignación y Transferencia de Créditos Académicos

mecanismos que permitan probar e incluso redefinir la seguridad implementada en las asignaturas mencionadas.
Intención didáctica
Los contenidos de los temas incluidos en esta asignatura, deben abordarse de tal forma que permitan una interacción reflexiva y funcional de los saberes. Partiendo del saber, saber hacer, saber ser y del saber transferir a distintos contextos del discente; es decir, primero adquirir el conocimiento, luego aplicarlo con ética y valores y posteriormente, lograr que esa práctica pueda trasladarse a diferentes ámbitos de la realidad del alumno. Lo anterior será el resultado de las actividades de aprendizaje que se enlistan. *El enfoque de ésta asignatura debe ser primordialmente práctico. Es deseable que los subtemas se aborden con profundidad, aunque sin perder de vista que el temario es extenso.* *El papel del docente consistirá en favorecer el cuestionamiento por parte de sus alumnos, con respeto y atención, facilitando la integración de habilidades de pensamiento con el fin de mejorar la capacidad de razonamiento, estimular la creatividad, contribuir al pensamiento inter e intrapersonal, desarrollar la comprensión ética y sobre todo facilitar el crecimiento de la capacidad que permita encontrar sentido a la experiencia.*

3.Participantes en el diseño y seguimiento curricular del programa

Lugar y fecha de elaboración o revisión	Participantes	Observaciones
Instituto Tecnológico de Zacatecas, septiembre de 2019.	Academia de Sistemas Computacionales e Informática	Definición y elaboración de los contenidos temáticos correspondientes a las asignaturas del módulo de la especialidad.
nstituto Tecnológico de Zacatecas, septiembre de 2019.	Academia de Sistemas Computacionales e Informática	Reunión de trabajo para el planteamiento general de los contenidos temáticos del módulo de especialidad.
nstituto Tecnológico de Zacatecas, septiembre de 2019.	Academia de Sistemas Computacionales e Informática	Reuniones para la definición y especificación de los contenidos temáticos, así como de la información complementaria requerida para las asignaturas del módulo de especialidad.

4.Competencias a desarrollar.

Competencia(s) específica(s) de la asignatura

1. Conoce y analiza la terminología básica del hacking ético con el objetivo de adentrarse en el área.
2. Conoce las habilidades que debe poseer un hacker para proporcionar seguridad en la empresa.
3. Conoce y aplica las metodologías Pentesting, practicando el ataque a diversos entornos, con la intención de descubrir fallas y vulnerabilidades.
4. Conoce y aplica herramientas para el reconocimiento de recursos de seguridad(footprinting) además de realizar pruebas de penetración para identificar los posibles seguimientos que se pueden llevar a cabo a un evento de intromisión.
5. Analiza e implementa el hackeo a las redes de datos, utilizando diversas técnicas, con el fin de identificar las vulnerabilidades en una red.
6. Conoce, analiza y aplica la variedad existente del software para hackeo así como las contramedidas necesarias, para identificar las áreas de oportunidad respecto a la seguridad de la organización.
7. Conoce, analiza y aplica las herramientas y contramedidas de otras técnicas de hackeo, para reducir la vulnerabilidad de la seguridad de la organización.
8. Analiza y aplica las pruebas básicas de penetración y evaluación de la seguridad organizacional, con el fin de garantizar mayor seguridad a la misma.

5.Conocimientos previos.

Identifica y aplica las características, estrategias y herramientas relativas a la seguridad informática a nivel usuario en un entorno de red de área local, con el fin de utilizar aplicaciones y herramientas que ayuden a mantener segura la red y los equipos personales en la misma.

Conoce el área de la Seguridad Perimetral para adentrarse en la terminología de la misma; además analiza el modelo de defensa en profundidad que lo lleva a identificar las capas que definen las técnicas y estrategias a aplicar en cada una.

6.Temario

Temas	Subtemas
Introducción al Hacking Ético	• Seguridad de la información. o Delitos en internet. o Conceptos de Hacking. o Tipos de ataque sobre un sistema o Importancia de tener un Ethical Hacking en la empresa. o Habilidades de un Hacker. o ¿Qué es Penetration testing? o Metodologías para realizar un Pentesting
Reconocimiento de recursos de seguridad (Footprinting)	• Definición y objetivos del Footprinting. • Herramientas Footprinting para realizar búsquedas. • Información de ubicación y de inteligencia competitiva. • WHOIS Lookup y extraer información de DNS. • Localizar rangos de red, traceroute y sitios web. • Extraer información de un sitio web. • Monitoreando actualizaciones web. • Seguimiento de comunicaciones de correo. • Footprinting usando técnicas de Google Hacking®. • Pentesting Footprinting.

Hackeo a Redes	•Escaneo y exploración de redes. o Escaneo de redes locales, direcciones IP, puertos abiertos y servidores. o Comprobación de sistemas activos con ICMP scanning. •Hackeo en redes inalámbricas. o Ataques a Access Point. o Metodología Wireless Hacking. o Metodología WarDriving. o Herramientas para romper WEP/WEPA y WarDriving. •Hackeo a servidores Web. o Tipos de ataques Web. o Metodología de ataque a servidor Web. o Pruebas de penetración. •Ataque a aplicaciones Web. o Tipos de ataques. o Arquitectura de Servicios Web. o Herramientas para hacking de aplicaciones Web.

Software para Hackeo	• Troyanos y BackDoors.
	  ○ Definición y tipos de troyanos.
	  ○ Canales Overt y Covert.
	  ○ Herramientas para detectar troyanos.
	  ○ Backdoors y contramedidas.
	• Virus y Gusanos.
	  ○ Tipos de virus y gusanos.
	  ○ Diferencia entre virus y gusanos.
	  ○ Detección de virus. contramedidas para virus y gusanos.
	• Sniffers.
	  ○ Conceptos de Sniffers.
	  ○ Funcionamiento de un Sniffers.
	  ○ Protocolos vulnerables Snifers.
	  ○ Envenenamientos MAC,ARP,DNS.
	  ○ Contramedidas MAC, ARP, DNS.

Otras Técnicas de Hackeo	• Denegación de Servicios (DoS).
	  ○ Ataque denegación de servicio.
	  ○ Botnet y herramienta de ataque DoS.
	  ○ Contramedidas DoS/DDoS.
	• Hijacking.
	  ○ Tipos de sesión Hijacking.
	  ○ Diferentes tipos de ataques.
	  ○ Número de secuencia TCP/IP Hijacking.
	  ○ Herramientas.
	• Inyección de instrucciones SQL.
	  ○ SQL Inyección.
	  ○ HTTP Post Request.
	  ○ Detección.
	  ○ SQL Inyección Black Box Pen Testing.
	  ○ Metodología.
	  ○ Herramientas para SQL Inyección.

Introducción a Pruebas de Penetración	• Tipos de Pruebas de Penetración. • Metodología. • Tipos de Pruebas. • Evaluación de seguridad de aplicaciones y de red. • Evaluación de Acceso remoto inalámbrico. • Evaluación de filtrado de red.

7.Actividades de aprendizaje de los temas

Introducción al Hacking Ético	
Competencias	Actividades de aprendizaje
Específica(s): 1. Conoce y analiza la terminología básica del hacking ético con el objetivo de adentrarse en el área. 2. Conoce las habilidades que debe poseer un hacker para proporcionar seguridad en la empresa. 3. Conoce y aplica las metodologías Pentesting, practicando el ataque a diversos entornos, con la intención de descubrir fallas y vulnerabilidades. Genéricas: **Competencias instrumentales** Capacidad de análisis y síntesis Capacidad de organizar y planificar Comunicación oral y escrita Habilidad para buscar y analizar información proveniente de fuentes diversas Solución de problemas Toma de decisiones Habilidad para utilizar el ordenador como herramienta de trabajo **Competencias interpersonales** Capacidad crítica y autocrítica Trabajo en equipo Habilidades interpersonales **Competencias sistémicas** Capacidad de aplicar los conocimientos en la práctica Habilidades de investigación Capacidad de aprender Capacidad de generar nuevas ideas (creatividad) Habilidad para trabajar en forma autónoma Búsqueda del logro Compromiso ético	1. Los alumnos realizarán consulta sobre los puntos de esta Unidad. 2. Se revisarán los conceptos consultados. 3. Se hará una discusión grupal de las implicaciones del hackeo y del concepto de Ética y su importancia en esta actividad. 4. Identificación de recursos de hackeo seguros y fuentes seguras de información, sin riesgo de estar quedando expuestos.

<table>
<tr><td>Preocupación por la calidad</td><td></td></tr>
<tr><td colspan="2">Reconocimiento de Seguridad (Footprinting)</td></tr>
<tr><td>Competencias</td><td>Actividades de aprendizaje</td></tr>
<tr><td>Específica(s):

1. Conoce y aplica herramientas para el rastreo de huellas (footprinting) además de realizar pruebas de penetración para identificar los posibles seguimientos que se pueden llevar a cabo a un evento de intromisión.

Genéricas:

Competencias instrumentales
Capacidad de análisis y síntesis
Capacidad de organizar y planificar
Comunicación oral y escrita
Habilidad para buscar y analizar información proveniente de fuentes diversas
Solución de problemas
Toma de decisiones
Habilidad para utilizar el ordenador como herramienta de trabajo

Competencias interpersonales
Capacidad crítica y autocrítica
Trabajo en equipo
Habilidades interpersonales

Competencias sistémicas
Capacidad de aplicar los conocimientos en la práctica
Habilidades de investigación
Capacidad de aprender
Capacidad de generar nuevas ideas (creatividad)
Habilidad para trabajar en forma autónoma
Búsqueda del logro
Compromiso ético
Preocupación por la calidad</td><td>1. Investigar las diferentes herramientas de reconocimiento de la seguridad (footprinting) identificando su área de uso, las ventajas y desventajas de las herramientas por área de aplicación (Internet, DNS, WebSite, Network, etc).
2. Identificar un objetivo y hacer Reconocimiento por: a) internet, b) WHOIS y DNS c) WebSite y Network d) Google hacking
3. Hacer reporte completo describiendo los pasos seguidos, las herramientas empleadas, las fuentes de información y de los recursos informáticos conseguidos, y los resultados obtenidos de esta actividad.
4. Investigar las contramedidas al footprinting, nivel de seguridad que provee cada una. Como configurar un firewall para evitar filtrar información, acciones contra DNS y WHOIS, personalizar errores para evitar dar información.</td></tr>
<tr><td colspan="2">3. Hackeo a Redes</td></tr>
<tr><td>Competencias</td><td>Actividades de aprendizaje</td></tr>
</table>

Específica(s): 1. Analiza e implementa el hackeo a las redes de datos, utilizando diversas técnicas, con el fin de identificar las vulnerabilidades en una red. Genéricas: **Competencias instrumentales** Capacidad de análisis y síntesis Capacidad de organizar y planificar Comunicación oral y escrita Habilidad para buscar y analizar información proveniente de fuentes diversas Solución de problemas Toma de decisiones Habilidad para utilizar el ordenador como herramienta de trabajo **Competencias interpersonales** Capacidad crítica y autocrítica Trabajo en equipo Habilidades interpersonales **Competencias sistémicas** Capacidad de aplicar los conocimientos en la práctica Habilidades de investigación Capacidad de aprender Capacidad de generar nuevas ideas (creatividad) Habilidad para trabajar en forma autónoma Búsqueda del logro Compromiso ético Preocupación por la calidad	1. E maestro presentará diferentes estrategias para realizar el escaneo de redes y la manera de aprovechar la información obtenida. 2. El alumno realizará una revisión de las herramientas de escaneo de redes, puertos abiertos y de direcciones Ip. Evaluará el nivel de confiabilidad del recurso encontrado y presentará las mejores herramientas y mas seguras de instalar en nuestra computadora sin riesgo de instalar un software malicioso. 3. El maestro presentará las debilidades de las redes inalámbricas, la forma de protegerlas y las herramientas para explotar las debilidades de las mismas. 4. El maestro presentará las debilidades de las aplicaciones web y las estrategias para protegernos y detectar la intromisión en nuestro sistema.
Software para Hackeo	
Competencias	Actividades de aprendizaje
Específica(s): 1. Conoce, analiza y aplica la variedad existente del software para hackeo así como las contramedidas necesarias, para identificar las	1. El maestro explicará el funcionamiento de los Troyanos y BackDoors, los mecanismos para lograr la intrusión o descarga en el objetivo, las formas de detección y de eliminación.

áreas de oportunidad respecto a la seguridad de la organización. Genéricas: **Competencias instrumentales** Capacidad de análisis y síntesis Capacidad de organizar y planificar Comunicación oral y escrita Habilidad para buscar y analizar información proveniente de fuentes diversas Solución de problemas Toma de decisiones Habilidad para utilizar el ordenador como herramienta de trabajo **Competencias interpersonales** Capacidad crítica y autocrítica Trabajo en equipo Habilidades interpersonales **Competencias sistémicas** Capacidad de aplicar los conocimientos en la práctica Habilidades de investigación Capacidad de aprender Capacidad de generar nuevas ideas (creatividad) Habilidad para trabajar en forma autónoma Búsqueda del logro Compromiso ético Preocupación por la calidad	2. El maestro explicará el funcionamiento de los Virus y Gusanos, los mecanismos para lograr la intrusión o descarga en el objetivo, las formas de detección y de eliminación. 3. El maestro explicará el funcionamiento de los Sniffers, los mecanismos para lograr la intrusión o descarga en el objetivo, las formas de detección y de eliminación. 4. Los alumnos realizarán la selección de las herramientas mejores y más confiables de cada uno de los tipos de software de este apartado.
Otras Técnicas de Hackeo	
Competencias	Actividades de aprendizaje
Específica(s): 1. Conoce, analiza y aplica las herramientas y contramedidas de otras técnicas de hackeo, para reducir la vulnerabilidad de la seguridad de la organización. Genéricas: **Competencias instrumentales** Capacidad de análisis y síntesis	1. El maestro explicará el objetivo de conseguir la Denegación de Servicios, las maneas de lograrlo y las contramedidas. 2. Los alumnos realizarán la investigación sobre el tema de Hijacking, objetivos, descripción, herramientas y contramedidas. 3. El maestro presentará la estrategia de Inyección de instrucciones SQL,

Capacidad de organizar y planificar Comunicación oral y escrita Habilidad para buscar y analizar información proveniente de fuentes diversas Solución de problemas Toma de decisiones Habilidad para utilizar el ordenador como herramienta de trabajo **Competencias interpersonales** Capacidad crítica y autocrítica Trabajo en equipo Habilidades interpersonales **Competencias sistémicas** Capacidad de aplicar los conocimientos en la práctica Habilidades de investigación Capacidad de aprender Capacidad de generar nuevas ideas (creatividad) Habilidad para trabajar en forma autónoma Búsqueda del logro Compromiso ético Preocupación por la calidad	su objetivo, resultados esperados, como realizarla y las contramedidas para evitarlas.
Introducción a Pruebas de Penetración	
Competencias	Actividades de aprendizaje
Específica(s): Analiza y aplica las pruebas básicas de penetración y evaluación de la seguridad organizacional, con el fin de garantizar mayor seguridad a la misma. Genéricas: **Competencias instrumentales** Capacidad de análisis y síntesis Capacidad de organizar y planificar Comunicación oral y escrita Habilidad para buscar y analizar información proveniente de fuentes diversas Solución de problemas Toma de decisiones	1. El maestro realizará la presentación de técnicas de penetración en sistemas. 2. Los alumnos realizarán la investigación de las herramientas disponibles para realizar las pruebas de penetración, las formas de lograrlo y las contramedidas correspondientes.

Habilidad para utilizar el ordenador como herramienta de trabajo **Competencias interpersonales** Capacidad crítica y autocrítica Trabajo en equipo Habilidades interpersonales **Competencias sistémicas** Capacidad de aplicar los conocimientos en la práctica Habilidades de investigación Capacidad de aprender Capacidad de generar nuevas ideas (creatividad) Habilidad para trabajar en forma autónoma Búsqueda del logro Compromiso ético Preocupación por la calidad	

8.Práctica(s).

1. Identificar un objetivo y hacer Reconocimiento por: a) internet, b) WHOIS y DNS c) WebSite y Network d) Google hacking. 2. Investigar las contramedidas al footprinting. Configurar un firewall para evitar filtrar información, realizar las medidas contra DNS y WHOIS, y configurar el sistema para evitar que trasciendan los errores y evitar dar información al respecto. 3. El alumno realizará el escaneo de alguna red, detectará puertos abiertos y direcciones Ip. 4. El alumno logrará brincar la seguridad de al menos dos tipos de redes inalámbricas usando software diferente para cada caso. 5. Lograr la infiltración de un Troyano o un Backdoor, además de un Virus o un gusano o un Sniffer. 6. Realizar la Inyección de instrucciones de SQL a un sistema.

9.Proyecto de asignatura.

El objetivo del proyecto que planteé el docente que imparta esta asignatura, es demostrar el desarrollo y alcance de la(s) competencia(s) de la asignatura, considerando las siguientes fases:

- **Fundamentación:** marco referencial (teórico, conceptual, contextual, legal) en el cual se fundamenta el proyecto de acuerdo con un diagnóstico realizado, mismo que permite a los estudiantes lograr la comprensión de la realidad o situación objeto de estudio para definir un proceso de intervención o hacer el diseño de un modelo.

- **Planeación:** con base en el diagnóstico en esta fase se realiza el diseño del proyecto por parte de los estudiantes con asesoría del docente; implica planificar un proceso: de intervención empresarial, social o comunitario, el diseño de un modelo, entre otros, según el tipo de proyecto, las actividades a realizar los recursos requeridos y el cronograma de trabajo.

- **Ejecución:** consiste en el desarrollo de la planeación del proyecto realizada por parte de los estudiantes con asesoría del docente, es decir en la intervención (social, empresarial), o construcción del modelo propuesto según el tipo de proyecto, es la fase de mayor duración que implica el desempeño de las competencias genéricas y especificas a desarrollar.

Evaluación: es la fase final que aplica un juicio de valor en el contexto laboral-profesión, social e investigativo, ésta se debe realizar a través del reconocimiento de logros y aspectos a mejorar se estará promoviendo el concepto de “evaluación para la mejora continua”, la metacognición, el desarrollo del pensamiento crítico y reflexivo en los estudiantes.

10.Evaluación por competencias.

Para evaluar las actividades de aprendizaje se recomienda solicitar: resúmenes, mapas conceptuales y/o mentales, exposiciones en clase, ensayos, reportes de visitas, cuestionarios resueltos, cuadro sinóptico, reportes de prácticas, reportes de estudios de casos y portafolio de evidencias.

Para verificar el nivel del logro de las competencias del estudiante se recomienda utilizar: listas de cotejo, listas de verificación, matrices de valoración, guías de observación, heteroevaluación, coevaluación y autoevaluación.

11. Fuentes de información

Harper, Allen, Harris, Shon, Ness, Jonathan, Eagle, Chris. Gray Hat Hacking The Ethical Hackers Handbook (2011), 3rd Edition. McGraw-Hill/Osborne Media

Simpson Michael T., Backman Kent, Corley James. Hands-On Ethical Hacking and Network Defense (2011). 1a Edición. Course Technology. Second Edition.

Accissi. (2011). *Seguridad Informática*. Ethical Hacking. Barcelona: ENI. 1a Edición.

Adam Olaf. (2007). *Seguridad en internet*. España: Marcombo S.A.2001. 1ra Edición.

Aguilera Lopez Purificacion. (2010). *Seguridad Informática*. España: Editex. 1ra Edición.

Alvarez Marañon Gonzalo. (2009). *Como protegernos de los peligros internet* España: Catarata.

Areitio Bertolin Javier. (2008). *Seguridad de la Información Redes, Informática y sistemas de Información*. España: Learning Paraninfo. 1ra Edición

Beekman George. (2004). *Introducción a la Informática*. Madrid: Pearson Educación. 1ra Edición

Corrales Hermoso Alberto Luis, Beltran Pardo Marta & Guzman Sacristan Antonio. (2006). *Diseño e Implantación de Arquitecturas Informáticas Seguras: Una Aproximación Práctica*. Madrid: Dykynson,S.L. 1ra Edición

De los Santos Sergio. (2009). *uno al dia. Once años de seguridad informática* Versión 2.0, http://hispasec.com/resources/UADv2.0.pdf

Garcia A & Alegre, M.P. (2011). *Seguridad Informática*. España: Paraninfo. 1ra 1ra Edición

Marroqui Nestor. (2010). *Tras los pasos de un Hacker*. Estados Unidos de Norte América: 1ra Edición.

Ramirez Lopez Dante Odin & Espinosa Madrigar Carmina Cecilia. (2011). El Cifrado Web (SSL/TLS) | Revista .Seguridad. Obtenido Septiembre 05, 2012, de revista.seguridad.unam.mx/numero-10/el-cifrado-web-ssltls

Sarubbi Juan Pablo. (2008). Seguridad Informática Técnicas de defensa comunes bajo variantes del sistema operativo Unix. Argentina: Universidad Nacional de Lujan

Tori Carlos (2008). Hacking Ëtico. Rosario, Argentina. Mastroianni Impresiones. 1ª Edición.